ABSTRACT OF THE DISCLOSURE

After an extended transformation of a plaintext, a reduced product-sum type encryption is carried out. The plaintext to be encrypted is divided thereby to obtain a plaintext vector. The plaintext vector is transformed by a predetermined function thereby to generate a transformation vector. Then, a ciphertext is generated by a product-sum operation between the components of a public key vector and the components of the plaintext vector and the transformation vector.